RECEIVED
CENTRAL FAX CENTER
JUL 28 2009

AMENDMENTS TO THE CLAIMS:

1. (previously presented): An electronic data storage system comprising:

a file device for storing at least electronic data; and

a data processing unit which generates a first check code for detecting falsification of said electronic data and a second check code for detecting falsification of a public key-based electronic signature using a secret encryption method and/or an encryption key when the electronic data is registered, stores said electronic data, said public key-based electronic signature, and said first and second check codes into said file device,

wherein said data processing unit generates said first check code by an encrypting method unique to said system from said electronic data, an electronic signature for registration by encrypting a hash value of said electronic data with a secret key, and said second check code by an encrypting method unique to said system from said electronic signature for registration, and

verifies the validity of said stored electronic data and said electronic signature by creating a third check code from said electronic data by said encrypting method unique to said system and a fourth check code from said electronic signature for registration by said encrypting method unique to said system, compares said stored first check code with said third check code and said stored second check code with said fourth check code, and outputs said electronic data, a second electronic signature created by encrypting said electronic data with a secret key which is valid at output time and said electronic signature for registration when said compared result is favorable.

2. (previously presented): An electronic data storage system comprising:

a file device for storing at least electronic data; and

a data processing unit which generates a check code for detecting falsification of a public key-based electronic signature using a secret encryption method and/or an encryption key when said electronic data is registered, stores said electronic data, said public key-based electronic signature and the falsification check code for said electronic signature into said file device, verifies the validity of said electronic signature using the check code attached to said electronic

signature and verifies the validity of said electronic data using said electronic signature when said electronic data is output, and then accesses said electronic data and said electronic signature when said validity is confirmed,

wherein said data processing unit generates an electronic signature for registration by encrypting a hash value of said electronic data with a secret key and generates said check code by a method unique to said system from said electronic signature for registration, and wherein said data processing unit verifies the validity of said stored electronic data by creating a second check code from said electronic signature for registration by said method unique to said system, and comparing said stored check code with said second check code, and outputs said electronic data, a second electronic signature created by encrypting said electronic data with a secret key which is valid at output time and said electronic signature for registration when said compared result is favorable.

3.-5. (canceled)

6. (previously presented): The electronic data storage system according to Claim 1, wherein said data processing unit stores a certificate of the public key with which said electronic signature was created, simultaneously along with said electronic signature into said file device, when said electronic signature is created.

7. (previously presented): The electronic data storage system according to Claim 6, wherein said data processing unit stores or outputs the expiration information of said public key certificate simultaneously.

8. (previously presented): The electronic data storage system according to Claim 2, wherein said data processing unit stores a certificate of the public key with which said electronic signature is created, simultaneously along with said electronic signature into said file device, when said electronic signature is created.

9. (previously presented): The electronic data storage system according to Claim 8, wherein said data processing unit stores or outputs the expiration information of said public key certificate simultaneously.

10. (previously presented): The electronic data storage system according to Claim 1, wherein said data processing unit creates a pair of said public key and said secret key according to a request for key creation, issues a request of issuing a public key certificate to a CA office, acquires a public key certificate, and stores said acquired public key certificate in said file device.

11. (currently amended): An electronic data storage method, implemented in an electronic data storage system further comprising a file device for storing at least electronic data and a data processing unit; the method comprising:

a step of generating an electronic signature for registration by encrypting a hash value of electronic data with a secret key;

a step of generating a first check code for detecting falsification of electronic data and a second check code for detecting falsification of a public key-based electronic signature using a secret-encryption method and/or an encryption-key method, said second check code being generated from said electronic signature for registration, when said electronic data is registered;

a step of storing said electronic data, said public key-based electronic signature, and said first and second check codes into a file device;

a step of respectively verifying the validity of said stored electronic data and said electronic signature using said first and second check codes attached to said stored electronic data and said electronic signature when said electronic data is output from said file device; and

a step of accessing said electronic data and said electronic signature when said validity is confirmed,

wherein said generating step comprises a step of generating said first and second check codes by a method unique to said system,

and wherein said verifying step comprises:

a step of creating a third check code from said electronic data and a fourth check code from said electronic signature for registration by said method unique to said system; and

a step of comparing said stored first check code with said third check code and said stored second check code with said fourth check code,

and wherein said accessing step comprises a step of outputting to a different device said electronic data, second electronic signature created by encrypting said electronic data with a secret key which is valid at output time and said electronic signature for registration when said compared result is favorable.

12. (canceled)

13. (currently amended): An electronic data storage method, implemented in an electronic data storage system further comprising a file device for stor ing at least electronic data and a data processing unit; the method comprising:

a step of generating an electronic signature for registration by encrypting a hash value of electronic data with a secret key;

a step of generating a check code for detecting falsification of a public key-based electronic signature using a secret-encryption method and/or an encryption-key method, when said electronic data is registered;

a step of storing said electronic data, said public key-based electronic signature, and said falsification check code for said electronic signature into a file device; and

a step of verifying the validity of said electronic data using said electronic signature after verifying the validity of said electronic signature using the check code attached to said electronic signature when said electronic data is output from said file device, and then accessing said electronic data and said electronic signature when said validity is confirmed,

wherein said generating step comprises a step of generating said check code by a method unique to said system from said electronic signature for registration,

and wherein said verifying step comprises:

a step of creating a second check code from said electronic signature for registration by said method unique to said system; and

a step of comparing said stored check code with said second check code; and

a step of outputting to a different device said electronic data, second electronic signature created by encrypting said electronic data with a secret key which is valid at output time and said electronic signature for registration when said compared result is favorable.

14. -15. (canceled)

16. (previously presented): The electronic data storage method according to Claim 11, wherein said storage step comprises a step of storing a certificate of the public key with which said electronic signature was created, simultaneously along with said electronic signature into said file device, when said electronic signature is created.

17. (previously presented): The electronic data storage method according to Claim 16, wherein said storage step comprises a step of storing a certificate of the public key with which said electronic signature was created, simultaneously along with said electronic signature, when said electronic signature is created.

18. (previously presented): The electronic data storage method according to Claim 11, wherein said storage or output step comprises a step of storing or outputting the expiration information of a public key certificate simultaneously.

19. (previously presented): The electronic data storage method according to Claim 11, further comprising:

a step of creating a pair of said public key and said secret key according to a request for the key creation;

a step of issuing a request of issuing a public key certificate to a CA office; and

a step of acquiring said public key certificate, and storing said public key certificate in said file device.

20. (previously presented): The electronic data storage method according to Claim 13, wherein said storage or output step comprise a step of storing or outputting the expiration information of a public key certificate simultaneously.

21. (previously presented): The electronic data storage method according to Claim 13, further comprising:

a step of creating a pair of said public key and said secret key according to a request for the key creation;

a step of issuing the request of issuing a public key certificate to a CA office; and

a step of acquiring said public key certificate, and storing said public key certificate in said file device.